Санкт-Петербургский государственный университет

 Γ руппа 23.M04-мм

Черников Артем Александрович

Реализация поиска оптимальных схем генерации запутанных состояний фотонов

Отчёт по производственной практике

Оглавление

В	ведение	3
1.	Постановка задачи	5
2.	Обзор	6
3.	Описание решения	7
	3.1. Математическая модель	7
	3.2. Расчёт верности	11
	3.3. Расчёт оповещения	12
	3.4. Градиентный спуск	13
4.	Результаты	15
	4.1. Генерация состояния GHZ	15
За	аключение	17
Ст	лисок литературы	18

Введение

Квантовые вычислительные устройства уже долгое время вызывают интерес у научного сообщества благодаря своей способности решать некоторые задачи намного быстрее, чем классические компьютеры [12, 15], тем самым демонстрируя так называемое квантовое превосходство. Впервые идея квантовых вычислений была предложена независимо Юрием Маниным и Ричардом Фейнманом в начале 1980-х [17, 19], но исследования в этой области начались ещё раньше [14]. С тех пор и по сей день активно рассматриваются способы создания квантовых компьютеров, а также открываются и изобретаются новые квантовые алгоритмы, то есть алгоритмы, исполняемые квантовым вычислительным устройством.

Одним из первых квантовых алгоритмов, демонстрирующих квантовое превосходство, является алгоритм Дойча-Джозы [5]. Впоследствии был предложен также алгоритм Бернштейна-Вазирани [1]. Несмотря на то что их практическое применение может вызывать сомнения, само их существование бросило вызов научному сообществу искать новые алгоритмы, демонстрирующие квантовое превосходство и решающие при этом более животрепещущие задачи.

Квантовый алгоритм, решающий очень важную задачу факторизации целого числа за полиномиальное время, был открыт американским учёным Питером Шором в 1994-м году [15]. На предположении о том, что такая задача нерешаема за обозримое количество времени, основаны многие даже современные криптосистемы. Отсюда стало ясно, что с помощью квантового компьютера можно взломать любую такую систему, и это открытие вызвало сильный интерес к квантовым компьютерам.

Спустя время в 1996-м году американский математик Лов Гровер изобрёл алгоритм поиска в неотсортированной базе данных [12], имеющий квадратичное ускорение по сравнению с лучшими известными классическими алгоритмами, решающими эту задачу. Алгоритм Гровера может быть использован для решения широкого спектра задач, в

частности, NP-полных задач.

Впоследствии американским физиком-теоретиком Дэвидом П. Ди-Винченцо были сформулированы критерии [4], которым должно соответствовать вычислительное устройство для того, чтобы по праву называться квантовым компьютером. Было предложено множество архитектур квантовых компьютеров: основанные на явлении ядерного магнитного резонанса; использующие электроны, запертые в квантовых точках; основанные на ядерных спинах идентичных молекул; использующие запутанные фотоны.

Идея создать квантовый компьютер на фотонах вызывает особый интерес благодаря тому, что практически все критерии ДиВинченцо выполнимы в этой архитектуре без особых усилий. Единственная трудность остаётся в осуществлении преобразований, запутывающих пару фотонов. Исследования в этой области на текущий момент привели к некоторым любопытным результатам [7, 11, 13], однако, к сожалению, все они не масштабируемы, и задача нахождения запутывающего преобразования остаётся открытой.

Одним из подходов к решению этой задачи является использование дополнительных фотонов, уже находящихся в специальном запутанном состоянии. Оказалось, что запутанность с них можно перенести на другие фотоны [11], и такие преобразования являются более эффективными по сравнению с теми, которые не используют изначальную запутанность вспомогательных фотонов. Оптические схемы, генерирующие фотоны в запутанных состояниях, крайне полезны для применения рассматриваемого подхода. Поиск наиболее эффективных среди них — актуальная задача.

Возникло предложение, что для поиска таких преобразований стоит использовать техники компьютерного поиска. Одним из классических таких подходов является градиентный спуск.

1. Постановка задачи

Целью данной работы является реализация поиска оптимальных схем генерации запутанных состояний фотонов.

Для достижения данной цели были поставлены следующие задачи.

- Расширить функциональность фреймворка galopy для поиска запутанных состояний.
- Произвести поиск схем генерации состояния GHZ.
- Проанализировать результаты и сделать выводы.

2. Обзор

Предпринималось множество удачных попыток сформулировать задачу поиска схемы как оптимизационную и реализовать результативный компьютерный поиск нужных параметров [10, 7, 8]. Описанные в статьях алгоритмы используют различные подходы к решению задачи поиска той или иной схемы, причем даже сама оптимизационная задача формулируется по-разному в разных статьях. При этом все алгоритмы объединяет то, что они подбирают параметры для оптических схем, максимизируя некую функцию потерь, семантически отражающую меру сходства текущей схемы с требуемой.

Рассматриваемые алгоритмы спроектированы и оптимизированы для поиска конкретной схемы, которая выполняет заданное преобразование. Замена искомого преобразования (или архитектуры схемы) вынуждена сопровождаться существенным редактированием исходного кода, что доставляет неудобства при решении задач.

Существующий поисковой фреймворк galopy¹ позволяет пользователю задавать в явном виде матрицу преобразования, которое требуется найти, а также архитектуру схемы от простой, состоящей только из оптических элементов и детекторов фотонов, до сложной, с множественными оповещениями и корректировками состояний после любого измерения. Эта гибкость предоставляет свободу для поиска нужной схемы, а также простоту добавления новой функциональности в код, поэтому было принято решение использовать этот фреймворк.

 $^{^{1}}$ Репозиторий проекта —
https://github.com/sysoevss/galopy (дата обращения: 11.06.2024)

3. Описание решения

В данном разделе представлено описание контекста решаемой задачи, технических подробностей и реализации решения. Код доступен в репозитории², размещённом на веб-сервисе GitHub.

3.1. Математическая модель

Согласно квантовой теории поля, фотон, как и некоторые другие элементарные частицы, способен пребывать в нескольких состояниях одновременно до тех пор, пока неопределённость относительно его состояния нисколько не влияет на окружающую его вселенную. Такое сложное состояние называется квантовой суперпозицией.

Как только состояние окружающей вселенной начинает зависеть от состояния фотона (например, состояние фотона детектируется датчиком), с точки зрения её жителей неопределенность состояния фотона исчезает. При этом фотон переходит из суперпозиции в какое-нибудь одно из возможных состояний с некоторой определённой вероятностью. Этот процесс называется коллапсом волновой функции частицы, или измерением состояния частицы.

В описанном выше примере фотон и его окружение до измерения представляли собой две независимые системы. После измерения одна система стала зависеть от другой, поэтому их теперь невозможно рассматривать по отдельности. Фотон и его окружение теперь являют собой единую неразделимую систему. С этой точки зрения коллапса волновой функции после измерения не произошло, вместо этого сама вселенная стала пребывать сразу в нескольких состояниях, причем жители вселенной из одного состояния никак не могут провзаимодействовать с ними же из другого состояния. Поэтому приверженцы этой теории, в парадигме которой в данной работе и рассматриваются физические явления, называют такии версии вселенных параллельными.

Аналогичным образом данные рассуждения переносимы с системы

 $^{^2}$ Репозиторий проекта —
https://github.com/sysoevss/galopy (дата обращения: 11.06.2024), пользователь artemgl

"фотон-окружение" на систему "фотон-фотон". Если состояние двух фотонов не представимо в виде двух независимых систем (по одной для каждого фотона), то эти фотоны находятся в так называемом запутанном состоянии, в котором состояние одного фотона зависит от состояния второго. Существенным отличием данного примера от предыдущего является процесс запутывания, — на практике перевести два фотона из незапутанного состояния в запутанное оказывается нетривиальной задачей.

Квантовый алгоритм в достаточно широком смысле представляет собой некоторое обратимое преобразование над системой, способной находиться в N различных состояниях. Для решения содержательных задач зачастую число N должно быть катастрофически большим, поэтому часто рассматриваются системы, состоящие из n подсистем, называемых кубитами, каждая из которых способна находиться всего в двух состояниях — $|0\rangle$ или $|1\rangle$. Тогда общее количество состояний зависит экспоненциально от количества простых подсистем (кубитов) и равно 2^n . Доказано [3, 6], что в такой архитектуре произвольное преобразование над всей системой представимо в виде последовательности однои двухкубитных преобразований (гейтов), причём среди двухкубитных достаточно наличие всего одного запутывающего гейта.

В данной работе рассматривается архитектура квантового компьютера на фотонах, называемая протоколом КLМ [11]. Каждый кубит кодируется ровно одним фотоном и парой пространственных мод, в которых может находиться этот фотон. Если он находится в первой моде, то состояние кубита считается равным $|0\rangle$, если во второй $-|1\rangle$.

Однокубитные преобразования в протоколе КLM осуществимы с помощью таких оптических элементов как фазовая пластина и светоделитель. Фазовая пластина имеет единственную входную и выходную моду и параметризуется всего одним углом, отвечающим за сдвиг фазы волновой функции проходящего через эту пластину фотона (рис. 1а). Светоделитель имеет два входных и два выходных плеча, что позволяет обеспечить взаимодействие двух мод между собой. Его принято параметризовать парой углов, один из которых отвечает за коэффици-

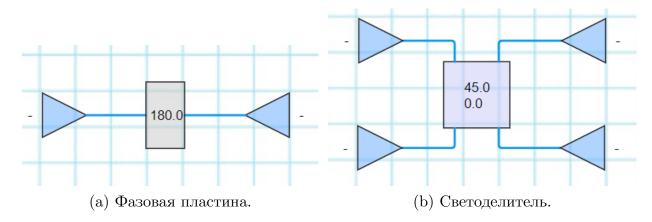


Рис. 1: Схематичные изображения оптических элементов, используемых в квантовой линейной оптике. Треугольниками обозначены источники и детекторы фотонов, линиями — моды, в которых могут находиться фотоны. Параметры оптических элементов (углы) указываются в градусах.

ент пропускания, а другой — за фазовый сдвиг после отражения или пропускания фотона. Так, если первый угол равен нулю, то светоделитель вырождается в идеальное зеркало, что эквивалетно отсутствию каких-либо оптических элементов; если же он равен 90°, то светоделитель наоборот пропускает все проходящие через него лучи, тем самым меняя фотоны в двух модах местами (рис. 1b).

Двухкубитный запутывающий гейт в протоколе КLМ неосуществим при помощи указанных выше оптических элементов. Однако исследования в этой области на данный момент пришли к тому, что с использованием дополнительных фотонов запутывающее преобразование становится осуществимо [7, 11]. Дополнительные фотоны взаимодействуют посредством оптических элементов с сигнальными (то есть теми, над которыми требуется произвести преобразование), после чего на дополнительных детекторах ожидается измерение определённого паттерна (к примеру, два фотона на первом датчике, один на втором и ноль на третьем). Считается, что гейт сработал правильно, тогда и только тогда, когда заданный паттерн оказался на датчиках в результате измерения. Измерение на дополнительных модах называется оповещением о работе гейта, а удачное измерение — правильным или верным оповещением.

Неотъемлемой частью гейтов с вышеописанной логикой работы яв-

ляется ненулевая вероятность неверного оповещения, что мешает использовать их на практике, поскольку для работы всего алгоритма, состоящего из сотен или тысяч таких гейтов, требуется, чтобы сработали все гейты до единого, вероятность чего оказывается крайне мала. Максимально известная на данный момент вероятность правильного оповещения одного гейта составляет 2/27 [7]. Использование вспомогательных фотонов в запутанном состоянии может сильно увеличить эту вероятность (теоретически — сколь угодно близко к единице [11]), поэтому возникает желание эффективно генерировать фотоны в запутанном состоянии.

Рассмотрим данную архитектуру подробнее. На вход гейта подаётся пара фотонов в некотором состоянии и несколько дополнительных фотонов, которые запускаются в дополнительные моды. Состояние, в котором находятся дополнительные фотоны, задано заранее и не зависит от состояния сигнальных фотонов. Сама схема представляет собой некоторым образом расставленные на всех модах оптические элементы с заданными углами. Также к схеме прилагается верное оповещение, ожидаемое на дополнительных модах. На выходе схемы в сигнальных модах ожидается пара фотонов в новом запутанном состоянии, получившемся в результате преобразования при верном оповещении.

Итак, преобразование, генерирующее фотоны в запутанном состоянии, в линейной квантовой оптике задаётся следующими параметрами.

- Количество дополнительных мод и состояние дополнительных фотонов, подаваемое на эти моды.
- Расстановка светоделителей и фазовых пластин на модах (далее
 топология преобразования).
- Углы (параметры) расставленных светоделителей и фазовых пластин.
- Измерение, считаемое за правильное оповещение.

Топология схемы может быть представлена как набор оптических элементов, поставленных последовательно друг за другом, где для каж-

дого из них указаны моды, на которых они действуют (один для фазовой пластины и два для светоделителя). Однако такое представление оказывается неудобным для использования на практике, а также избыточным. Эквивалентными преобразованиями любая схема может быть приведена к виду последовательности лишь светоделителей, после которых следуют фазовые пластины по одной на каждую моду. В связи с этим для удобства представления топологии схемы рассматривается только расстановка светоделителей, а фазовые пластины в конце преобразования всегда подразумеваются.

Вышеперечисленных параметров достаточно для однозначного определения оптической схемы, среди которых требуется найти такую, которая генерирует состояние GHZ^3 с максимально возможной вероятностью правильного оповещения (ниже приведён вид этого состояния в нотации Дирака: три фотона находятся либо одновременно в состоянии $|0\rangle$, либо одновременно в состоянии $|1\rangle$). Выбор именно этого состояния обусловлен тем, что оно очень часто используется в запутывающих схемах [9]. Для решения этой задачи был применён градиентный спуск. После этого были проанализированы результаты.

$$|GHZ\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

3.2. Расчёт верности

Верность преобразования — это мера, отражающая, насколько одно преобразование похоже на другое. Во время поиска гейта верность требуется для оценки того, насколько точно имеющаяся схема реализует заданное искомое преобразование.

Способы задания верности гейтов основаны на верности, определённой на отдельных состояниях. Мерой схожести (верностью) двух состояний между собой принято считать квадрат их скалярного произ-

 $^{^3}$ Статья про состояние GHZ — https://en.wikipedia.org/wiki/Greenberger%E2%80%93Horne%E2%80%93Zeilinger_state (дата обращения: 11.06.2024)

ведения.

$$F(|\varphi\rangle, |\psi\rangle) = |\langle \varphi|\psi\rangle|^2$$

Эта мера может быть перенесена на гейты с помощью идеи, описанной в статье [16] и заключающейся в подсчёте средней верности между ожидаемым и полученным состоянием по всему пространству. Формула для её вычисления выглядит следующим образом.

$$F(U,V) = \int_{S^{2n-1}} |\langle \psi | V^{\dagger} U | \psi \rangle|^2 dV =$$

$$= \frac{1}{n(n+1)} \Big(Tr(MM^{\dagger}) + |Tr(M)|^2 \Big),$$
 где $M = V^{\dagger}U$

Записью M^{\dagger} обозначена эрмитово сопряжённая к M матрица; число n — количество столбцов или строк квадратной матрицы M. Из вида формулы можно заметить, что основная её вычислительная сложность заключается в двух матричных произведениях.

3.3. Расчёт оповещения

Состояние на выходе схемы описывает полную суперпозицию расположений фотонов, получившуюся в результате их прохождения через оптические элементы. Для того, чтобы расчитать преобразование, реализуемое схемой, и вероятность срабатывания гейта, нужно вычислить состояние в сигнальных модах, оказавшееся в результате коллапса волновой функции при верном оповещении. Это происходит путём редуцирования всего пространства на соответствующее подпространство.

Аналогично расчёту верности, описанному в разделе 3.2, было принято решение вычислять среднюю вероятность по всему пространству. Формула вероятности верного оповещения принимает следующий вид (средний скалярный квадрат вектора, полученного после преобразования).

$$P(U) = \int_{S^{2n-1}} \langle \psi | U^{\dagger} U | \psi \rangle dV = \frac{1}{n} Tr(U^{\dagger} U)$$

Поскольку от произведения матриц U^{\dagger} и U сразу берётся след, пол-

ностью считать это произведение не нужно. Для вычисления следа достаточно просуммировать все элементы матрицы, полученной в результате поэлементного умножения U^{\dagger} на U, что и было использовано в реализации.

3.4. Градиентный спуск

Условия применимости градиентного спуска заключаются в дифференцируемости функции потерь, из чего возникает требование наличия только вещественных параметров. Препятствием к применению этого метода выступает то, что многие параметры, задающие оптическую схему, целочисленны.

Однако это препятствие удалось обойти путём избавления от таких параметров как топология схемы и верное оповещение. Оставшиеся целочисленные параметры были вынесены в так называемые гиперпараметры, то есть настраиваемые вручную, перед запуском алгоритма поиска.

Существуют топологии схем, в которых возможно задать любое унитарное преобразование, меняя только углы закреплённых на своих местах оптических элементов [2, 18]. Назовём такие топологии универсальными. Таким образом, если зафиксировать некоторую универсальную топологию схемы, пространство поиска нисколько не сузится. В качестве универсальной топологии рассматривалась параллельная топология (рис. 2), поскольку она лучше всех себя показала при предыдущих экспериментах.

После нескольких запусков функция потерь была подобрана следующим образом. Аргументы функции р и f — соответственно массив вероятностей верного оповещения и массив верностей преобразования. Под индексом i в каждом массиве находится информация об i-том верном оповещении. Параметры f_min и p_min означают соответственно минимальные приемлемые верность и вероятность работы гейта. Параметр n_measurements означает количество допустимых верных оповещений.

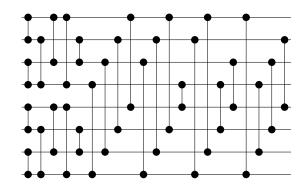


Рис. 2: Параллельная топология схемы для восьми мод. Горизонтальными линиями обозначены моды. Каждый вертикальный отрезок представляет собой светоделитель, действующий на модах, отмеченных жирными точками.

```
def loss(p, f):
loss_value = 0
for i in range(n_measurements):
  fidelity = f[i]
  probability = p[i]
  if probability > p_min:
      loss_value += fidelity
  else:
      loss_value += 1 + probability
  return loss value
```

Таким образом, в процессе работы алгоритма в первую очередь настраиваются наиболее приемлемые верности для всех оповещений, после чего параметры обновляются в направлении повышения вероятностей всех оповещений. Также можно заметить, что алгоритм максимизирует функцию потерь, в отличие от классического подхода, в котором она минимизируется. Концептуально это изменение ни на что не влияет.

4. Результаты

В данном разделе представлены результаты поиска генерации состояния GHZ. Все эксперименты проводились в среде выполнения Google Colab⁴ с поддержкой графического процессора.

4.1. Генерация состояния GHZ

Запуск алгоритма поиска производился в двух архитектурах (с одним и с двумя оповещениями) со следующими параметрами.

- Количество градиентных шагов: 4000.
- Приемлемая вероятность верного оповещения: 1/108 для одного оповещения и 1/54 для двух.
- Количество вспомогательных мод: 4.
- Количество вспомогательных фотонов: 3.

Наилучшая известная схема, генерирующая фотоны в состоянии GHZ, имеет вероятность 1/54 [10]. Эта схема имеет два оповещения, то есть срабатывает верно, если на вспомогательных модах был измерен любой из двух заданных паттернов. Каждое из оповещений имеет вероятность реализоваться, равную 1/108. Алгоритм поиска успешно справился с задачей поиска схемы с одним оповещением, но для двух оповещений нашел схему с максимальной верностью около 0.88. Это может быть связано с тем, что в оригинальной схеме из статьи [10] не применяется корректировка состояния после измерения паттерна, в отличие от схем, среди которых производился поиск в данной работе. Корректировка состояния даёт шанс найти более оптимальную схему, но при этом существенно увеличивает количество настраиваемых параметров, усложняя поиск. Возможно, именно отказ от корректировки позволит найти оптимальную схему. Ещё одним решением проблеки позволит найти оптимальную схему.

 $^{^4\}mathrm{C}$ тартовая страница с описанием среды выполнения Google Colab — https://colab.research.google.com (дата обращения: 11.06.2024)

мы может выступить последовательная настройка параметров: сначала для самого преобразования, затем для корректировок.

Заключение

В ходе выполнения данной работы были достигнуты следующие результаты.

- Расширена функциональность фреймворка galopy для поиска запутанных состояний.
- Произведены попытки поиска схем генерации состояния GHZ.
- Проанализированы результаты, сделаны выводы.

Код доступен в репозитории⁵, размещённом на веб-сервисе GitHub.

 $^{^5}$ Репозиторий проекта —
https://github.com/sysoevss/galopy (дата обращения: 11.06.2024), пользователь artemgl

Список литературы

- [1] Bernstein E. Vazirani U. Quantum complexity theory. 1993. Access mode: https://dl.acm.org/doi/pdf/10.1145/167088.167097 (online; accessed: 11.06.2024).
- [2] Clements W.R. et al. Optimal design for universal multiport interferometers. 2016. Access mode: https://opg.optica.org/optica/fulltext.cfm?uri=optica-3-12-1460 (online; accessed: 11.06.2024).
- [3] D.P. DiVincenzo. Two-bit gates are universal for quantum computation.—1995.—Access mode: https://arxiv.org/pdf/cond-mat/9407022.pdf (online; accessed: 11.06.2024).
- [4] D.P. DiVincenzo. The physical implementation of quantum computation. 2000. Access mode: https://arxiv.org/pdf/quant-ph/0002077.pdf (online; accessed: 11.06.2024).
- [5] Deutsch D. Jozsa R. Rapid solution of problems by quantum computation. 1992. Access mode: https://www.isical.ac.in/~rcbose/internship/lectures2016/rt08deutschjozsa.pdf (online; accessed: 11.06.2024).
- [6] Deutsch D.E. Barenco A. Ekert A. Universality in quantum computation.—1995.—Access mode: https://arxiv.org/pdf/quant-ph/9505018.pdf (online; accessed: 11.06.2024).
- [7] E. Knill. Quantum gates using linear optics and postselection.— 2002.—Access mode: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.66.052306 (online; accessed: 11.06.2024).
- [8] Fldzhyan S.A. Saygin M.Y. Kulik S.P. Compact linear optical scheme for Bell state generation. 2021. Access mode: https://journals.aps.org/prresearch/pdf/10.1103/PhysRevResearch.3.043031 (online; accessed: 11.06.2024).

- [9] Gimeno-Segovia M. Shadbolt P. et al. From Three-Photon Greenberger-Horne-Zeilinger States to Ballistic Universal Quantum Computation. 2015. Access mode: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.115.020502 (online; accessed: 11.06.2024).
- [10] Gubarev F.V. Dyakonov I.V. et al. Improved heralded schemes to generate entangled states from single photons. 2020. Access mode: https://arxiv.org/pdf/2004.02691 (online; accessed: 11.06.2024).
- [11] Knill E. Laflamme R. Milburn G.J. A scheme for efficient quantum computation with linear optics. 2001. Access mode: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=7955e6b51070395b97b70ddb8d7e2ae797528a81 (online; accessed: 11.06.2024).
- [12] L.K. Grover. A fast quantum mechanical algorithm for database search. 1996. Access mode: https://dl.acm.org/doi/pdf/10. 1145/237814.237866 (online; accessed: 11.06.2024).
- [13] O'Brien J.L. et al. Demonstration of an all-optical quantum controlled-NOT gate. 2003. Access mode: https://arxiv.org/pdf/quant-ph/0403062.pdf (online; accessed: 11.06.2024).
- [14] P. Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. 1980. Access mode: https://link.springer.com/article/10.1007/BF01011339 (online; accessed: 11.06.2024).
- [15] P.W. Shor. Algorithms for disquantum computation: and factoring. — 1994. — Access mode: logarithms crete https://citeseerx.ist.psu.edu/document?repid=rep1&type= pdf&doi=2273d9829cdf7fc9d3be3cbecb961c7a6e4a34ea (online; accessed: 11.06.2024).

- [16] Pedersen L.H. Møller N.M. Mølmer K. Fidelity of quantum operations. 2007. Access mode: https://arxiv.org/pdf/quant-ph/0701138.pdf (online; accessed: 11.06.2024).
- [17] R.P. Feynman. Simulating physics with computers. 1982.
- [18] Reck M. et al. Experimental realization of any discrete unitary operator. 1994. Access mode: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.73.58 (online; accessed: 11.06.2024).
- [19] Ю.И. Манин. Вычислимое и невычислимое. 1980.